УДК 343.98

Д. И. Шнейдерова
преподаватель кафедры уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

ОБЫСК ПО УГОЛОВНЫМ ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ: ТАКТИЧЕСКИЕ И ПРОЦЕССУАЛЬНЫЕ ПРОБЛЕМЫ

Тактика проведения следственного действия приобретает свои специфические особенности, отличные от общих выработанных наукой и практикой рекомендаций, в зависимости от вида и способа совершенного преступления. Хищения в сфере оборота криптовалют — относительно молодая группа преступлений (регистрируются с 2018 г.), при расследовании которых проведение отдельных следственных действий вызывает затруднения у сотрудников органов следствия и дознания по причинам недостаточности специальных знаний в данной области, отсутствия типовых тактических рекомендаций по рассматриваемой группе хищений, а также наличия связанных с этими причинами проблем процессуального характера, вызванных пробелами уголовно-процессуального законодательства. В этой связи представляется необходимым выделение особенностей тактики проведения одного из следственных действий по делам о хищениях в сфере оборота криптовалют, вызывающего затруднения, — обыска.

Обыск по делам о хищениях в сфере оборота криптовалют — неотложное следственное действие, проводимое, как правило, на последующем этапе расследования и направленное на поиск и изъятие объектов и цифровых следов, имеющих доказательственное значение для расследуемого уголовного дела, в рамках обследования помещений, иных мест или лиц. Так как хищения в сфере оборота криптовалют относятся к компьютерным преступлениям, то, как правило, во всех случаях обыск направлен на поиск технических устройств — носителей цифровых доказательств (компьютеры, ноутбуки, планшеты, смартфоны, съемные накопители данных, аппаратные криптокошельки, установочные флешки и оптические диски). При этом уже на подготовительном этапе важно понимать, в каком состоянии с точки зрения выполнения рабочих процессов могут быть обнаружены такие устройства. Если отключенные устройства трудностей не вызывают, поскольку беспроблемно изымаются для дальнейшего исследования, то работающие (для съемных носителей — подключенные к компьютеру), к тому же с активным интернет-соединением и/или выполняющие определенные программные процессы, могут потребовать незамедлительных действии, направленных на сохранение данных. При описанных выше обстоятельствах возникает тактическая необходимость в участии специалиста, обладающего

знаниями в сфере информационных и сетевых технологий, а также имеющего практический опыт работы с криптовалютными сервисами, чье содействие позволит быстро зафиксировать имеющую значение информацию. Приглашая специалиста, следователь (лицо, производящее дознание) должен удостовериться, что последний имеет необходимое техническое и программное оснащение для работы с компьютерной информацией (ее копирования, создания образа носителя).

Следует отметить, что белорусское уголовно-процессуальное законодательство предоставляет органу уголовного преследования право выбора относительно участия специалиста при производстве следственных действий. Однако с точки зрения криминалистической тактики при производстве обыска по делам о хищениях криптовалют целесообразность его обязательного участия при каждом случае вызвана несколькими причинами: во-первых, направляясь к месту проведения обыска, следователь (лицо, производящее дознание) не обладает достоверными сведениями о состоянии технических объектов, которые могут быть обнаружены, следовательно, необходимость привлечения специалиста к участию предугадать наверняка невозможно; во-вторых, если в ходе проведения обыска все же выяснится, что следователь (лицо, производящее дознание) не сможет самостоятельно обнаружить и копировать компьютерную информацию с устройства и для этого все же нужно пригласить специалиста, то обыск придется завершить (поскольку его приостановление не предусмотрено уголовно-процессуальным законодательством), а затем вынести постановление о проведении повторного обыска и санкционировать его у прокурора, что займет время и может привести к уничтожению и потере данных.

Кроме того, неотложность обыска и специфика преступления побуждают орган предварительного расследования в рамках подготовительного этапа действовать быстро, следовательно, поиск и сбор таких участников, как специалист и понятые, должны происходить также быстро, что не всегда практически возможно. Если к понятым не предъявляются особые требования по уровню и отрасли их знаний, в связи с чем обеспечение их присутствия проблем не вызывает, то со специалистом дела обстоят иначе, особенно в небольших городах, где по профилю информационных технологий они отсутствуют вовсе либо их количество незначительно и не обеспечивает нужды следствия. Представляется, что при расследовании хищений в сфере оборота криптовалют следователю надлежит заранее (на первоначальном этапе расследования) наладить контакт с несколькими специалистами соответствующего профиля в целях возможности быстрого обеспечения их присутствия в качестве участника следственного действия, проводимого неотложно. Также данная мера позволит в рамках сотрудничества привлекать одного и того же специалиста к участию в разных следственных действиях или консультированию, что обеспечит осведомленность

специалиста о необходимых для его работы обстоятельствах уголовного дела и не потребует потери времени на их разъяснение, позволит быстро сориентироваться при обыске, в каком направлении следует искать требуемую информацию и как проводить ее фиксацию и копирование.

Еще одна проблема процессуального характера может возникнуть при необходимости осмотра компьютерной информации (в частности, активных ресурсов, имеющих возможность удаленного доступа) на устройствах, обнаруженных в ходе обыска. К примеру, в ходе обыска обнаружен ноутбук, на котором запущен браузер и осуществлен вход в онлайн-криптокошелек или аккаунт социальной сети / мессенджера. Предупреждая возможность перевода криптовалют на иной кошелек сообщником подозреваемого, у которого могут иметься необходимые данные для авторизации, или удаления чатов и иных сведений из социальных сетей (для отдельных мессенджеров / социальных сетей характерен режим исчезающих сообщений, которые через небольшой промежуток времени удаляются сервисом), лицо, производящее обыск, должно незамедлительно провести осмотр данной компьютерной информации, зафиксировать вебстраницы путем производства скриншотов или фотографирования, для криптовалют — наложить на них арест. По мнению Л. Л. Мельника, в подобных случаях обыск необходимо приостановить, провести осмотр компьютерной информации и наложить арест на криптовалюту (если обнаружен активный кошелек и есть сведения для доступа к нему) [1, с. 149]. Целесообразность данного пути с точки зрения тактики сомнений не вызывает, и в этом с автором следует согласиться, однако уголовно-процессуальная возможность для таких действий на сегодняшний день не предусмотрена.

Часть 13^1 ст. 210 Уголовно-процессуального кодекса Республики Беларусь (далее — УПК) предусматривает, что при проведении обыска допустимо копирование компьютерной информации в отображаемой форме (в том числе создание образа носителя) при невозможности или нецелесообразности изъятия объекта, ее содержащего [2]. Исходя из этого положения, проводить осмотр криптовалютного кошелька и налагать арест на криптовалюту подозреваемого в ходе обыска, так же как и приостанавливать его для этих целей, — незаконно, т. к. не предусмотрено УПК. Также вызывает вопросы возможность копирования отображаемой информации. Если подходить к этому буквально, то получается, что лицо, производящее обыск, может произвести копирование только того рабочего окна, которое уже открыто на устройстве, либо же путем присоединения своих аппаратно-технических средств к устройству подозреваемого создать образ его системы или жесткого диска, при этом никаких иных манипуляций производиться не должно.

Однако на практике возникают ситуации, когда необходимо незамедлительно осмотреть содержимое устройства, аккаунт социальной сети, личный кабинет банкинга, транзакции кошелька, аккаунт криптобиржи и т. д. в связи с возможностью удаленного доступа к этой информации и ее искажения либо уничтожения. Для этих целей понадобится предварительный осмотр компьютерной информации, имеющейся на устройстве, путем просмотра содержимого жестких дисков, активации программ, в том числе для доступа к криптокошельку, открытие браузера и переход к аккаунту социальной сети и т. д., что уже выходит за рамки копирования, предусмотренного ст. 210 УПК. Кроме того, копирование допустимо в случаях, если изъять устройство невозможно или нецелесообразно, однако в большинстве случаев (что прослеживается и на практике) потребуется не только осмотреть компьютерную информацию в режиме неотложности, но и изъять после этого само устройство, так как на нем может быть обнаружена иная, имеющая значение для дела информация, в рамках экспертизы получен доступ к зашифрованным или удаленным файлам, на само устройство также может налагаться арест для обеспечения возмещения причиненного преступлением вреда. Таким образом, при необходимости осмотра компьютерной информации на устройствах, обнаруженных при обыске, согласно действующему УПК, последовательность действий следующая:

– Обыск необходимо прекратить, о чем составить протокол.

– Инициировать осмотр компьютерной информации. Если предполагаемая к осмотру информация будет связана с частной жизнью лица и будет подпадать под требования ч. 2 ст. 204^1 УПК, то потребуется согласие и присутствие обладателя этой информации, которое он может и не дать, поскольку, как правило, обыск проводится у подозреваемого, не желающего сотрудничать со следствием себе во вред. В этой ситуации необходимо вынести постановление на проведение осмотра предмета и компьютерной информации, без санкции прокурора, что вызвано неотложностью и допустимо указанной выше нормой УПК.

– Для изъятия осмотренного устройства потребуется провести повторный обыск с вынесением постановления без санкции прокурора по тем же причинам (ч. 3 ст. 210 УПК).

– Уведомить надзирающего прокурора о проведении осмотра и обыска без его санкции с обоснованием причин.

Видится, что такой алгоритм времязатратный и требует подготовки большого числа документов. Кроме того, при данной последовательности отсутствует возможность одновременного осмотра компьютера с содержащейся на нем информацией и производства поисковых действий в рамках обыска. Например, такая ситуация актуальна в случае, когда на устройстве обнаружен криптокошелек, но подозреваемый отказывается предоставить данные для доступа к нему.

Для отыскания данных авторизации одновременно специалистом может исследоваться содержимое файлов устройства, а иными участниками (привлеченными лицами, осуществляющими дознание) обыск в помещении или подозреваемого для отыскания носителей с записью такой информации (блокноты, стикеры, тетради, листы бумаги, флешки и т. д.).

В научной литературе встречается точка зрения, что исследование и копирование компьютерной информации в ходе обыска являются не осмотром, а составной частью обыска, поскольку на устройстве производятся поисковые действия. Однако с таким утверждением трудно согласиться, так как при обыске поисковые действия производятся в помещениях, иных местах или у лиц, что вытекает из ст. 208 УПК, а компьютер (иное техническое устройство) обозначить в качестве места затруднительно, поскольку его цифровое содержимое не обладает теми пространственными границами определенного места или характеристиками лица. Кроме того, если все же принять данную точку зрения за истину, то проведение осмотра компьютерной информации не в связи с обыском ничем по своей сущности не будет отличаться от поисковых действий на компьютере при обыске, следовательно, получится, что действие одно и то же — просмотр содержимого накопителя с целью обнаружения значимой для следствия информации, а процессуально именуется по-разному и предусмотрено двумя разными следственными действиями, что недопустимо.

Таким образом, резюмируя вышеизложенное, можно прийти к следующим выводам:

1. Исходя из специфики объектов поиска по делам о хищениях в сфере оборота криптовалют, для работы с которыми на месте могут потребоваться специальные знания в сфере информационных технологий, в частности функционирования криптовалютных сервисов и программ, видится тактически целесообразным в обязательном порядке приглашать специалиста к участию во всех случаях проведения обыска по делам рассматриваемой категории. Количественный недостаток таких специалистов может быть компенсирован образованием специализированных подразделений в структуре криминалистических отделов Следственного комитета Республики Беларусь, кадровое комплектование которых необходимо обеспечивать кандидатами, имеющими высшее образование с соответствующей целям и задачам подразделений квалификацией (программист, инженер-программист, системный аналитик, специалист по кибербезопасности), а также практический опыт работы по данному направлению.

2. В целях обеспечения процессуальной возможности проведения осмотра компьютерной информации в процессе производства обыска (одновременность вызвана тактическими соображениями и порождает комплексность данных следственных действий при исключительных обстоятельствах) представляется

целесообразным внести дополнение в ст. 210 УПК путем введения ч. 13^2 следующего содержания: в случаях, не терпящих отлагательства, а также при необходимости наложения ареста на криптовалюту, принадлежащую подозреваемому, обвиняемому, в соответствии с требованиями статьи 132 настоящего Кодекса, при производстве обыска может одновременно проводиться осмотр компьютерной информации по правилам, предусмотренным частью 3^1 статьи 204, статьей 204^1 настоящего Кодекса.

---

1. Мельник Л. Л. О некоторых аспектах рабочего этапа обыска при расследовании преступлений, совершенных с использованием токенов и электронных денег // Вестн. Акад. МВД Респ. Беларусь. 2022. № 1. С. 147–152. Вернуться к статье

2. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс] : 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 09.03.2023 г. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье